Amendments To Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-17 (cancelled).

18. (currently amended) An online card present transaction method comprising ~~the steps of~~:

~~receiving, at a host website, an HTTP request from a client computer of a user, said request having been redirected from a website of a merchant to said host website;~~

~~interrogating said client computer for the presence of an authentication device;~~

detecting, from a host system, the presence of a smart card reader connected to a client computer;

presenting to a user a payment option for using a smart card for payment;

receiving, from said client computer, a selection by said user of said payment option;

~~sending said user~~ transmitting, to said client computer, a challenge string in response to said selection by said user, wherein said challenge string prompts said user to insert a smart card into said smart card reader, wherein said smart card stores a digital certificate ~~when said client computer includes an authentication device~~;

receiving, at said host system, a copy of said digital certificate and a signed challenge string from said client computer, after said user enters a Personal Identification Number (PIN) which triggers signing of said challenge string and accessing said digital certificate;

authenticating, at said host system, said smart card ~~user by receiving authentication information from said user, wherein said authentication information corresponds to a transaction account of said user~~ using said signed challenge string and said copy of said digital certificate;

generating, at said host system, a secondary transaction account number, wherein said secondary transaction account number is valid for a single purchase transaction;

associating, at said host system, said secondary transaction account number with said transaction account of said user; and,

~~establishing an authenticated communication channel via an authentication process between a host system and said merchant; and~~

communicating, by said host system, said secondary transaction account number over said authenticated communication channel to ~~said~~ a merchant, wherein said merchant submits a payment request based on said secondary transaction account number.

19. (previously presented) The method of claim 18, wherein said authentication process comprises the steps of:

embedding an encrypted host system signature in said client computer of said user; and

redirecting a browser of said client computer to said merchant, causing said merchant to authenticate said host system by decrypting said host system signature.

20. (previously presented) The method of claim 18, wherein said authentication process comprises the steps of:

communicating a token to said merchant over a first communication channel;

receiving a communication from said merchant over a second communication channel requesting said host system to confirm issuance of said token; and

confirming to said merchant that said host system issued said token.

Claims 21-22 (cancelled).

23. (currently amended) An online-card-present transaction method comprising ~~the steps of~~:

communicating with a ~~user~~ client computer over a distributed network;

detecting the presence of a smart card reader connected to said client computer;

presenting a user of said client computer with a payment option for using a smart card for payment;

~~interrogating a computer system for the presence of an authentication device~~;

receiving a selection by said user of said payment option;

redirecting said ~~user~~ client computer to a website of a host system ~~website~~ in response to said detection; ~~when said client computer includes said authentication device,~~ wherein said host system:

transmits a challenge string to said client computer, wherein said challenge string prompts said user to insert said smart card into said smart card reader, wherein said smart card stores a digital certificate;

receives a copy of said digital certificate and a signed challenge string from said client computer, after said user enters a Personal Identification Number (PIN) which triggers signing of said challenge string and accessing said digital certificate;

~~authenticate~~ authenticates said ~~user~~ smart card using said signed challenge string and said copy of said digital certificate ~~based on data extracted from a transaction instrument by said authentication device~~;

generates ~~generating~~ a secondary transaction account number, wherein said secondary transaction account number is valid for a single purchase transaction;

associates ~~associating~~ said secondary transaction account number with an account of said user; and,

~~establishing an authenticated communication channel with said host system;~~

communicates ~~communicating~~ said secondary transaction account number ~~over said authenticated communication channel~~ to said ~~user~~ client computer, wherein said user of said client computer submits a payment request based on said secondary transaction account number; and,

receiving account information including said secondary transaction account number from said host system over said authenticated communication channel, wherein said account information and said secondary transaction account number facilitates completion of a transaction between said user and a merchant.

24. (previously presented) The method of claim 23, wherein said step of generating said secondary transaction account number comprises the steps of:

receiving an encrypted host system signature; and

decrypting said encrypted host system signature to determine that said account information originated with said host system.

25. (currently amended) The method of claim 23, ~~said~~ further comprising:

establishing an authenticated communication channel; ~~step further comprising the steps of:~~

receiving a host system token over a first communication channel, wherein said token identifies said host system; and

communicating to said host system over a second communication channel to confirm that said token was issued by said host system.

Claims 26-34 (cancelled).

35. (currently amended) An online card-present transaction method, comprising ~~the steps of~~:

~~establishing an authenticated communication channel;~~

~~receiving from~~ transmitting to a merchant computer ~~over said authenticated communication channel, a user~~ a request to facilitate a transaction with a merchant;

~~interrogating said merchant computer for the presence of an authentication device;~~

receiving a payment option for using a smart card for payment in response to said merchant computer detecting a presence of a smart card reader connected to a client;

transmitting a selection by said user of said payment option;

receiving a challenge string in response to said selection;

receiving a prompt from said challenge string to insert said smart card into a smart card reader, wherein said smart card stores a digital certificate;

~~communicating to said merchant computer a challenge string to facilitate a user authentication process when said merchant computer includes an authentication device;~~

~~retrieving from said merchant computer at least one of: a signed challenge string and a digital certificate originating from a user, wherein said user is authenticated by comparing said at least one of: said signed challenge string and said digital certificate to data corresponding to said user;~~

entering a Personal Identification Number (PIN) which triggers signing of said challenge string to create a signed challenge string and which accesses said digital certificate;

transmitting a copy of said digital certificate and said signed challenge string to a host computer, wherein said host computer:

authenticates said smart card using said signed challenge string and said copy of said digital certificate;

retrieves ~~retrieving~~ a primary transaction account number associated with said digital certificate;

generates ~~generating~~ a secondary transaction account number, wherein said secondary transaction account number is valid for a single purchase transaction;

associates ~~associating~~ said secondary transaction account number with said primary transaction account number; and

provides ~~providing~~ said secondary transaction account number to said merchant computer, wherein said merchant computer submits a payment request based on said secondary transaction account number.

Claim 36 (cancelled).

37. (previously presented) The method of claim 35, further comprising the steps of:

receiving said secondary transaction account number from said merchant computer as part of a settlement process; and,

applying a charge associated with said settlement process to a transaction account of said user associated with said secondary account transaction number.